Amendments to the Claims

Claim 1 (previously presented): A security container that secures a document component by encapsulating, within the security container, an encrypted version of the document component, an encrypted version of conditional logic for controlling operations on the document component, and key distribution information usable for controlling access to the document component, wherein:

the encrypted version of the document component and the encrypted version of the conditional logic are both encrypted using a first key;

the key distribution information comprises at least two key elements; and

each key element comprises (i) an identification of a user, a user group, a process, or a process group that is authorized to access the document component; and (ii) an encrypted version of the first key, wherein the encrypted version of the first key comprises the first key encrypted using a second key that is usable only by the identified user, user group, process, or process group for decrypting the encrypted version of the first key, thereby enabling that user, user group, process, or process group to obtain the first key and use it for decrypting the document component and the conditional logic.

Claim 2 (previously presented): The security container according to Claim 1, wherein the document component comprises a portion of a higher-level document and the security container secures the portion of the higher-level document.

Claim 3 (original): The security container according to Claim 2, wherein the higher-level document has more than one portion secured by security containers.

Claim 4 (previously presented): A method of securing document content using security containers, comprising the step of encapsulating, within a security container, an encrypted version of a document component, an encrypted version of conditional logic for controlling operations on the document component, and key distribution information usable for controlling access to the document component, wherein:

the encrypted version of the document component and the encrypted version of the conditional logic are both encrypted using a first key;

the key distribution information comprises at least two key elements; and

each key element comprises (i) an identification of a user, a group of users, a process, or group of a processes that is authorized to access the document component; and (ii) an encrypted version of the first key, wherein the encrypted version of the first key comprises the first key encrypted using a second key that is usable only by the identified user, user group, process, or process group for decrypting the encrypted version of the first key, thereby enabling that user, group of users, process, or groups of processes to obtain the first key and use it for decrypting the document component and the conditional logic.

Claim 5 (canceled)

Claim 6 (previously presented): The method according to Claim 4, wherein the first key comprises a symmetric key.

Claim 7 (previously presented): The method according to Claim 6, wherein the second key comprises, for each of the key elements, a public key associated with the identified user, process, group of users, or group of processes.

Claim 8 (canceled)

Claim 9 (original): The method according to Claim 4, wherein the conditional logic further controls access to the document component.

Claim 10 (original): The method according to Claim 9, wherein the key distribution information further controls access to the conditional logic.

Claim 11 (canceled)

Claim 12 (original): The method according to Claim 4, wherein the security container is encoded in structured document format.

Claim 13 (original): The method according to Claim 12, wherein the structured document format is Extensible Markup Language ("XML") format.

Claim 14 (canceled)

Claim 15 (previously presented): The method according to Claim 4, wherein at least one of the key elements identifies a group of users and wherein the users in the group are determined dynamically, upon receiving a request to access to the document component.

Claim 16 (previously presented): The method according to Claim 15, wherein the dynamic determination further comprises accessing a repository where the users in the group are identified.

Claim 17 (previously presented): The method according to Claim 4, further comprising the steps of:

receiving, from a requester, a request to access the document component;

programmatically determining, using the key distribution information, whether the requester is authorized to access the document component by determining whether, in any selected one of the key elements, the requester is the identified user or the identified process or is a member of the identified group of users or the identified group of processes, and if so, performing steps of:

decrypting the encrypted version of the first key from the selected one of the key elements using the second key usable by that requester, thereby obtaining the first key;

decrypting the encrypted version of the conditional logic using the first key, thereby obtaining the conditional logic;

decrypting the encrypted version of the document component using the first key, thereby obtaining the document component; and

programmatically evaluating, using the conditional logic, whether the request can

be granted; and

rejecting the request when the programmatically determining step has a negative result.

Claim 18 (original): The method according to Claim 17, wherein the conditional logic evaluates at least one of: an identity of the requester; a device used by the requester; a context of the requester; a zone of an application used by the requester; a user profile of the requester; and a target destination of the request.

Claim 19 (previously presented): A computer program product for securing document content using security containers, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code for receiving, from a requester, a request to access document content, wherein the document content is encapsulated as an encrypted version of a document component within a security container along with an encrypted version of conditional logic for controlling operations on the document component and key distribution information usable for controlling access to the document component, wherein:

the encrypted version of the document component and the encrypted version of the conditional logic are both encrypted using a first key;

the key distribution information comprises at least two key elements; and

each key element comprises (i) an identification of a user, a group of users, a process, or group of a processes that is authorized to access the document component; and (ii) an encrypted version of the first key, wherein the encrypted version of the first key comprises the

first key encrypted using a second key that is usable only by the identified user, user group, process, or process group for decrypting the encrypted version of the first key, thereby enabling that user, group of users, process, or groups of processes to obtain the first key and use it for decrypting the document component and the conditional logic;

computer-readable program code for programmatically determining, using the key distribution information, whether the requester is authorized to access the document component by determining whether, in any selected one of the key elements, the requester is the identified user or the identified process or is a member of the identified group of users or of the identified group of processes, and if so, performing steps of:

decrypting the encrypted version of the first key from the selected one of the key elements using the second key usable by that requester, thereby obtaining the first key;

decrypting the encrypted version of the conditional logic using the first key, thereby obtaining the conditional logic;

decrypting the encrypted version of the document component using the first key, thereby obtaining the document component; and

programmatically evaluating, using the conditional logic, whether the request can be granted; and

computer-readable program code for rejecting the request when operation of the computer-readable program code for programmatically determining yields a negative result.

Claim 20 (previously presented): A system for securing document content using security containers, comprising:

a security container that encapsulates an encrypted version of a document component, an encrypted version of conditional logic for controlling operations on the document component, and key distribution information usable for controlling access to the document component, wherein:

the encrypted version of the document component and the encrypted version of the conditional logic are both encrypted using a first key;

the key distribution information comprises at least two key elements; and

each key element comprises (i) an identification of a user, a group of users, a process, or group of a processes that is authorized to access the document component; and (ii) an encrypted version of the first key, wherein the encrypted version of the first key comprises the first key encrypted using a second key that is usable only by the identified user, user group, process, or process group for decrypting the encrypted version of the first key, thereby enabling that user, group of users, process, or groups of processes to obtain the first key and use it for decrypting the document component and the conditional logic;

means for receiving, from a requester, a request to access the document component;

means for programmatically determining, using the key distribution information, whether the requester is authorized to access the document component by determining whether, in any selected one of the key elements, the requester is the identified user or the identified process or is a member of the identified group of users or of the identified group of processes, and if so, performing steps of:

decrypting the encrypted version of the first key from the selected one of the key elements using the second key usable by that requester, thereby obtaining the first key;

decrypting the encrypted version of the conditional logic using the first key,

thereby obtaining the conditional logic;

decrypting the encrypted version of the document component using the first key, thereby obtaining the document component; and

programmatically evaluating, using the conditional logic, whether the request can be granted; and

means for rejecting the request when operation of the means for programmatically determining yields a negative result.

Claim 21 (original): The system according to Claim 20, wherein the security container is embedded within a document.

Claim 22 (original): The system according to Claim 20, wherein the security container encapsulates the document component on a system clipboard.

Claim 23 (original): The system according to Claim 20, wherein the security container is placed on a user interface.

Claim 24 (original): The system according to Claim 20, wherein the security container encapsulates the document component for exchange using interprocess communications.

Claim 25 (original): The system according to Claim 20, wherein the security container encapsulates the document component for exchange using a messaging system.

Claim 26 (original): The system according to Claim 20, further comprising means for copying the document component to a target destination, wherein the means for copying copies the entire security container in order to copy the document component.

Claims 27 - 32 (canceled)

Claim 33 (new): The method according to Claim 4, wherein the encrypted version of the first key in each key element is further encrypted using a secret key known to code implementing the security containers.

Claim 34 (new): The method according to Claim 4, wherein the encrypted version of the first key in each key element is encrypted using a secret key known to code implementing the security containers instead of using the second key, and the second key is then used to further encrypt a result of encrypting the first key using the secret key.